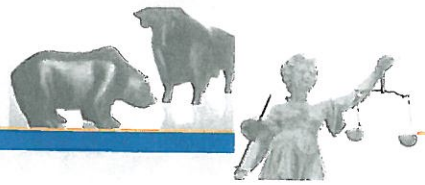

Digitale Zahnarztpraxis

Eine Zahnarztpraxis rein analog zu führen ist zumindest für Kassenzahnärzte seit dem 1. Januar 2012 unmöglich geworden – seit diesem Tag sind Sie verpflichtet, alle erbrachten vertragszahnärztlichen Leistungen papierlos mit ihrer kassenzahnärztlichen Vereinigung abzurechnen. Doch auch ohne diesen Zwang werden immer mehr Bereiche in den Zahnarztpraxen digitalisiert.

Claudia Göpfert

Sei es, dass die Buchhaltung intern elektronisch geführt wird, die Terminverwaltung am PC den Papierkalender ersetzt oder auch komplette Patientenakten digital erstellt werden und die medizinischen Unterlagen wie beispielsweise Röntgenbilder auf diesem Weg gespeichert werden. Doch, was ist zu beachten? Herausforderungen müssen nicht nur bei der Wahl der Praxissoftware (I) und der rein digital geführten Patientenakte (II) gemeistert werden. Auch die Sicherung (III) und die Sicherheit (IV) der Daten spielen eine große Rolle.

Claudia Göpfert

/// PRAXISSOFTWARE

Bereits bei der Wahl der Praxissoftware sollten Sie sorgfältig vorgehen. Sie sollten bei Ihrer Entscheidung berücksichtigen, ob die Software alle erforderlichen und von Ihnen gewünschten Funktionen bietet und später um Funktionen erweitert werden kann. Außerdem sollten Sie und Ihre Mitarbeiter die Software gut bedienen können. Ebenfalls sollten Serviceleistungen angeboten werden, beispielsweise eine Hotline, die Ihnen bei Fragen und Problemen zur Seite steht, und ein Update-Service, der die Software auf dem neuesten Stand hält.

Wenn mehrere Zahnärzte in einer Praxis dieselbe Software mit identischem Datenbestand nutzen, muss die Software auch die Herausforderung bewältigen können, die die Schweigepflicht an sie stellt. Dass nämlich Patientenakten nur von dem Zahnarzt eingesehen werden können, um dessen Patient es sich tatsächlich handelt. Dies ist besonders wichtig, wenn ein potenzieller Nachfolger in die Praxis eintritt, wenn mehrere eigenständige Zahnärzte in einer Praxisgemeinschaft tätig sind oder ein Patient in einer Gemeinschaftspraxis darauf besteht, nur mit einem Zahnarzt einen Behandlungsvertrag zu schließen.

Eine weitere Anforderung an die Software ergibt sich, wenn Sie mit der kassenzahnärztlichen Vereinigung abrechnen wollen. Dies beschränkt Sie in der Wahl, welche Praxissoftware Sie einsetzen.

Software, mit der der Vertragszahnarzt Leistungen zum Zweck der Abrechnung erfasst, speichert und verarbeitet, muss durch die zuständige kassenzahnärztliche Vereinigung genehmigt werden. Sie als Zahnarzt müssen dann bei jeder EDV-Abrechnung bestätigen, dass die genehmigte Programmversion verwendet wurde. Informieren Sie sich also am Besten vorher bei der Kassenzahnärztlichen Bundesvereinigung, ob Ihre Wunschsoftware als geeignet befunden wurde.

/// DIGITALE PATIENTENAKTEN

Ein weiterer zentraler Punkt, und zwar im Hinblick auf die digitale Führung der Patientenakten, ist die Anforderung an die Dokumentation.

So könnten Patienten im Haftungsprozess einwenden, die elektronische Patientenkarteikarte, insbesondere digitale Röntgenbilder oder die Datei, mit der die Aufklärung dokumentiert wird, seien nachträglich verfälscht worden. Man kann sich darüber streiten, ob hier tatsächlich größere Bedenken angebracht sind als gegenüber Patientenkarteikarten aus Papier. Denn auch wenn unterschiedliche Schriftfarben gut erkennbar sind, ist nicht ausgeschlossen, dass ein Zahnarzt immer mit dem gleichen Stift schreibt und so unerkannt Ergänzungen vornimmt. Die Hemmschwelle ist sicherlich nicht größer, als ein digitales Dokument nachträglich zu bearbeiten.

Außerdem gibt es mittlerweile mehrere Urteile, mit denen entschieden wurde, dass eine EDV-Dokumentation, die nicht gegen nachträgliche Veränderung gesichert ist, dennoch den vollen Beweiswert wie eine übliche handschriftliche Dokumentation hat, wenn der Zahnarzt plausibel darlegt, dass die Dokumentation nicht nachträglich verändert wurde und die Dokumentation auch aus medizinischen Gesichtspunkten plausibel erscheint (OLG Hamm, Urteil vom 26. Januar 2005, Az.: 3 U 161/04; OLG Naumburg, Urteil vom 26.01.2012 – 1 U 45/11). Liegen allerdings Anhaltspunkte für eine nachträgliche Fälschung vor – beispielsweise wenn die Art der Dokumentation deutlich von dem sonstigen Aufklärungsumfang abweicht – neigen die Gerichte eher dazu, den Anspruch stattzugeben (OLG Köln, Urteil vom 25.11.2013 – 5 U 164/12).

Unterlagen, die in einem Haftungsprozess einen Beweiswert haben können, sollten Sie daher mit einer qualifizierten elektronischen Signatur versehen. Werden digitale Röntgenbilder nachträglich mit einem Bildbearbeitungsprogramm verändert, beispielsweise aufgehellt oder in Ausschnitten vergrößert, sollte sowohl die Ursprungsversion als auch das bearbeitete Bild mit einer solchen Signatur versehen werden.Aufgrund des technischen Fortschrittes wachsen die Anforderungen an beweissichere Signaturen übrigens beständig. Auch Signaturen, die an-

gesichts der heutigen Technik als rechtssicher anerkannt sind, können möglicherweise schon im nächsten oder übernächsten Jahr gefälscht werden. Gemessen an der Archivierungsdauer ist dies ein verhältnismäßig kurzer Zeitraum. Sie sollten daher die elektronische Signatur jedes einzelnen Dokuments rechtzeitig erneuern, um die Beweiskraft digitaler Signaturen zu erhalten.

/// DATENSICHERUNG

Wenn Sie Ihre Daten digital verwalten, sollten Sie ebenfalls für eine regelmäßige Datensicherung sorgen, denn allzu schnell gehen digitale Daten verloren.
Grundsätzlich gibt es zwei Wege, wie die Daten gesichert werden können. Neben der Sicherung auf Hardware wie USB-Stick oder externen Festplatten, die in den Praxisräumen durchgeführt wird, bieten mehrere Anbieter mittlerweile auch Online-Datensicherungen an. Angesichts der sensiblen Daten ist von der Nutzung solcher Dienste abzuraten. Sie können nie sicher sein, ob die Datenübertragung gesichert ist und wer auf die Daten Zugriff erlangen kann.
Auch im Hinblick auf die Häufigkeit der Datensicherung gibt es Vorgaben. Die Gerichte fordern bei Unternehmern mindestens tägliche Datensicherungen (OLG Hamm, Urteil vom 01. Dezember 2003, 13 U 133/03) und zusätzlich vor der Installation von neuen Programmen. Wenn Sie Patientenakten rein digital führen, erscheint dies gerade im Hinblick auf den haftungsrechtlichen Aspekt und die Anzahl der pro Tag behandelten Patienten sehr wenig. Wird nur einmal am Tag eine Datensicherung durchgeführt, können alle Einträge in den Patientenakten des Tages verloren gehen. Diese werden nur sehr schwer wieder zu beschaffen sein. Hier empfiehlt sich sogar eine kontinuierliche Datensicherung, also eine Datensicherung, die ausgeführt wird, wobei Änderungen umgehend gesichert werden können.

Für die Datensicherung sollten Sie mehrere Datenträger im Wechsel verwenden, sodass die letzte Sicherung vom Tag davor nicht direkt überschrieben wird. Falls die neu aufgespielte Sicherungsdatei defekt ist oder der ganze Datenträger unbenutzbar wird, haben Sie sonst das Problem, das Ihnen alle Sicherungen auf einmal verloren gehen.
Die Datenträger sollten Sie regelmäßig an einem anderen Ort als der Praxis lagern, da diese bei einem Diebstahl oder Brand verloren gehen können. Geeignet ist dafür ein feuerfester Tresor bzw. ein Bankschließfach.

/// DATENSICHERHEIT

Der bei Weitem wichtigste Punkt, den Sie bei der digitalen Verwaltung beachten sollten, ist der Datenschutz. Dieser beginnt bereits beim Aufstellen und Einrichten der Hardware.
So sollten die Räume, in denen die Rechner stehen, immer dann verschlossen sein, wenn die Anlagen unbewacht sind. Stehen die Rechner in Räumen, zu denen die Patienten Zugang haben, stellen Sie sicher, dass keine Anschlüsse (z.B. USB) vorhanden sind, die zugänglich sind und genutzt werden können, um Daten zu stehlen. Idealerweise sind auch die Rechner, auf denen Patientendaten liegen, nicht mit dem Internet verbunden.
Die Bildschirme sollten in allen Räumen so ausgerichtet werden, dass die Patienten weder beim Gespräch noch beim Betreten oder Verlassen des Raumes direkten Blick auf diesen haben. Auf jedem Rechner sollte ein Bildschirmschoner installiert sein, der nur durch Eingabe eines – sicheren – Passwortes die Rückkehr zur Arbeitsoberfläche gewährt. Ihre Mitarbeiter sollten Sie anweisen, beim Verlassen des Arbeitsplatzes den Bildschirmschoner stets zu aktivieren – am einfachsten wird dies gehen, wenn eine Tastenkombination eingerichtet wird, die den Bildschirmschoner startet. Für den Fall,

Anzeige

dass dies einmal vergessen wird, sollte ein kurzer Zeitraum eingerichtet werden, in dem sich der Bildschirmschoner selbst aktiviert.

Daneben sollten Sie den Virenschutz auf allen Rechnern aktuell halten und eine Firewall installieren. Wenn die Rechner, auf denen Patientendaten verarbeitet werden, zugleich mit dem Internet verbunden sind, sollten Sie zusätzlich eine Hardware-Firewall, zum Beispiel einen zwischengeschalteten Router, verwenden. Sie sollten Ihre Rechner auch so einrichten, dass nicht jeder Mitarbeiter selbstständig Software installieren kann. So minimieren Sie das Risiko von schädlicher Software.

Speziell für E-Mail-Programme ist zu beachten, dass Nachrichten nicht automatisch geöffnet und Nachrichten, in denen Patientendaten übermittelt werden, geeignet verschlüsselt werden. So können verdächtige Mails möglicherweise von vornherein aussortiert werden. Erst recht sollten Dateianhänge nur geöffnet werden, wenn das Antivirenprogramm dies geprüft hat. Dies gilt auch, wenn der E-Mail-Anhang von einem Ihnen bekannten Absender stammt und von Ihnen erwartet wird – wenn fremde Rechner mit schädlicher Software infiziert sind, kann diese – vom Versender unbemerkt – die Datei verändert haben, um sich weiter zu verbreiten.

Dies sind einfache Grundregeln, die – wenn Sie alle Daten intern bearbeiten – bereits einen großen Teil der Gefahren ausräumen. Doch wenn die eigene Rechnerkapazität nicht reicht, wird teilweise auf Speicherplatz in einem externen Rechenzentrum zurückgegriffen, wo die Patientendaten dann verarbeitet werden. Auch einige Programme, beispielsweise Programme, bei denen der Patient über Ihre Homepage die verfügbaren Termine abfragen und seinen Wunschtermin vereinbaren kann, verarbeiten die Daten zumeist auf den eigenen Servern.

Zudem gehen immer mehr Softwarehersteller dazu über, ihre Software nicht mehr zu verkaufen, sodass sie auf den Rechnern der Zahnarztpraxis installiert werden und vor Ort genutzt werden kann, ohne dass Daten nach außen gegeben werden müssen, sondern bieten ihre Produkte im Rahmen eines sogenannten „Software-as-a-Service"-Vertrags an. Bei dieser Gestaltung wechseln Sie den Rechner, sobald Sie die Programmmaske aufrufen. Sie geben die Daten nicht auf Ihrem Rechner ein, sondern arbeiten über eine Verbindung auf dem Rechner des Anbieters. Wenn die betroffene Software nur funktioniert, wenn eine Verbindung zum Internet besteht, können Sie ziemlich sicher davon ausgehen, dass es sich um einen solchen Service handelt.

Rechtlich gesehen handelt es sich hierbei um eine sogenannte Auftragsdatenverarbeitung. Diese ist in § 11 Bundesdatenschutzgesetz geregelt und nur unter bestimmten Voraussetzungen zulässig und führt dazu, dass Sie für die Datenverarbeitung verantwortlich bleiben.

Das Gesetz schreibt hierfür vor, dass Sie den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen und den Auftrag schriftlich erteilen müssen. Weiter gibt es konkrete Vorgaben, was der schriftliche Vertrag alles regeln muss.

Seriöse Anbieter, die einen solchen Service anbieten, werden hier nicht nur auf eine sichere Datenverbindung und einen guten Schutz der EDV-Anlage achten, sondern auch Musterverträge für diese Auftragsdatenverarbeitung bereithalten und Ihnen konkret mitteilen können, welche technischen und organisatorischen Maßnahmen ergriffen wurden (beispielsweise, mit Schloss und Alarmanlagen gesicherte Serverräume, umsichtige Auswahl der Mitarbeiter, Verschwiegenheitsverpflichtung der Mitarbeiter). Da Sie für die Datenverarbeitung nach dem Gesetz in vollem Umfang verantwortlich sind und Verstöße gegen das Datenschutzgesetz und erst recht die zahnärztliche Schweigepflicht massiv geahndet werden, sollten Sie hier besondere Sorgfalt walten lassen.

/// DATENSCHUTZBEAUFTRAGTE

Ein weiterer Umstand, der häufig zu wenig beachtet wird, ist das Erfordernis eines Datenschutzbeauftragten, dessen Aufgabe es ist, in der Praxis auf die Einhaltung des Datenschutzes hinzuwirken. Gemäß § 4f Bundesdatenschutzgesetz müssen Sie einen Beauftragten für den Datenschutz schriftlich bestellen, wenn nicht in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Wenn also mindestens 10 Personen mit der Datenverarbeitung beschäftigt sind, müssen Sie einen Datenschutzbeauftragten bestellen. Dies kann einer Ihrer Mitarbeiter sein oder auch ein externer Datenschutzbeauftragter. Übrigens kommt es nicht darauf an, ob die Mitarbeiter in Voll- oder Teilzeit angestellt sind, oder ob einzelne Mitarbeiter nur mit Vor- oder Nacharbeiten (z.B. Versenden der Ausdrucke) beschäftigt sind.

/// FAZIT

Die digitale Zahnarztpraxis bietet viele Möglichkeiten, aber auch einige Stolperfallen. Eine umfassende Darstellung der zu beachtenden Punkte ist nahezu unmöglich. Zögern Sie nicht, bei der Einrichtung Ihrer Hardware kompetenten technischen und rechtlichen Rat von Ansprechpartnern einzuholen, die sich nicht nur auf die Beratungsbereiche, sondern auch auf Zahnärzte als Kundengruppe spezialisiert haben. Denn diese wissen um die besonderen Anforderungen, vor denen Sie stehen.

AUTOR
Claudia Göpfert
Rechtsanwältin
Fachanwältin für gewerblichen Rechtsschutz
Fachanwältin für Urheber- und Medienrecht

KONTAKT
LYCK & PÄTZOLD.
medizinanwälte
Lyck & Pätzold Medizinanwälte
Nehringstraße 2
61352 Bad Homburg
Telefon: 06172/13 99 60
Telefax: 06172/13 99 66
E-Mail: kanzlei@medizinanwaelte.de
Internet: www.medizinanwaelte.de